United States District Court

EASTERN DISTRICT OF OKLAHOMA

In the matter of the search of:	**Case No.** 21-MJ-402-SPS
Information That is Stored at Premises Controlled by Google	

APPLICATION FOR SEARCH WARRANT

I, Special Agent Christopher Worshek, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the **NORTHERN** District of **CALIFORNIA** *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A": This court has authority to issue this warrant under Title 18, United States Code, Sections 2703(c)(1)(A) and 2711(3)(A).

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Section(s) 1111(a), 1151, and 1153, and the application is based on these facts:

☐ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christopher Worshek
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed.

Date: October 22, 2021

Judge's signature

City and state: Muskogee, Oklahoma

UNITED STATES MAGISTRATE JUDGE
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE	Case No. 21-MJ-402-SPS

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Christopher Worshek, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Title 18, United States Code, Section 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Google to disclose to the government the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information and seize the information described in Section II of Attachment B.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI), and have been so employed since July 9, 2017. I am currently assigned to the Oklahoma City Division, Muskogee RA of the FBI. Prior to being assigned to Muskogee, I was assigned to the FBI Violent Crime Squad of the Jackson Division. Prior to being employed as a Special Agent with the FBI, I

practiced law for approximately five years. As a Special Agent with the FBI, I am a law enforcement officer of the United States as defined by Title 18, United States Code, Section 2510(7), meaning that I am empowered by law to investigate violations of Federal law, including violations of the Major Crimes Act (MCA), Title 18, United States Code, Section 1153, make arrests, and execute warrants issued under the authority of the United States. During my time as a Special Agent, I have participated in numerous criminal investigations as the primary investigator. I have also received significant training in criminal investigations.

3. The statements contained in this Affidavit are based in part on: information provided by other law enforcement and criminal justice agencies, including written reports of other law enforcement agents, witness statements, and/or court records that I have received, directly or indirectly, from other law enforcement agents; independent investigation; and my experience, training, and background as a Special Agent with the FBI. Because this Affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of the investigation. In addition, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part.

4. Based on the facts set forth in this affidavit, there is probable cause to believe JERRY LEE MATLOCK, JR. committed the offense of Murder in Indian Country in violation of Title 18, United States Code, Sections 1111, 1151, and 1153. There is also probable cause to search the information described in Attachment A for evidence of the crime as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by Title 18, United States Code, Section 2711. Specifically,

the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." Title 18, United States Code, Section 2711(3)(A)(i).

6. The facts and circumstances alleged in this affidavit occurred within the Eastern District of Oklahoma. More specifically, 474531 East 823rd Road, Stilwell, Oklahoma is within the geographic boundaries of the Cherokee Nation Reservation, and therefore is within Indian Country. JERRY LEE MATLOCK, JR. is an enrolled member of the Cherokee Nation and has some degree of Indian blood.

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

7. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

8. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet ("wi-fi") access points if a user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

9. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-

range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect.

10. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

11. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

12. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.*, Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed-in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed-in to a Google account.

13. In addition, based on my training and experience, I know Google offers an Internet

browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

14. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

15. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a] service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. Location History is stored on Google servers, and is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

16. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of

error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point.

17. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

18. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information

can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

19. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

20. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

21. During the evening of September 14, 2021, the Adair County Sheriff's Department responded to a shooting incident at 474531 East 823 Road, Stilwell, Oklahoma. Robert "Bob" Scraper was discovered outside of his residence suffering from a fatal gunshot wound.

22. Scraper lived at the residence, along with JERRY LEE MATLOCK, JR., who has been indicted by a federal grand jury for murdering Scraper in Indian Country. MATLOCK regularly drove a dark blue Dodge Ram pickup truck bearing a Cherokee Nation license plate.

23. Before the shooting, C.S. arrived at the residence on a motorcycle. According to R.C., who was already at the residence, Scraper asked MATLOCK to move MATLOCK's truck so that C.S. could park in the driveway to put air in a tire. MATLOCK got into his truck and left. According to C.S., MATLOCK was not at the home when C.S. arrived, but instead came running down the road from the east. When Scraper asked MATLOCK what was wrong, MATLOCK stated that he was getting out of here. MATLOCK then drove off in the pickup truck.

24. C.S. put air in his motorcycle tires and was backing out of the driveway when a dark colored truck with round headlights slowly pulled up around the curve of the roadway. The truck backed up to turn around and drove away slowly. C.S. heard a loud boom, which he initially thought was a tire blowing out, saw Scraper grab his chest, and heard Scraper say I think they killed me. Scraper then fell to the ground.

25. R.C., who was on the porch when C.S. started the motorcycle, heard what he thought was a backfire that sounded like a pistol being fired. R.C. saw headlights to the west of the driveway and saw the vehicle back out and head north on 4745 Road towards Highway 51.

26. According to a review of surveillance video from near the incident, at approximately 8:30:54 p.m., what appears to be a pickup truck leaves the general area of Scraper's

residence. At approximately 8:43:41 p.m, what appears to be a pickup truck drives toward the general area of Scraper's residence. At approximately 8:44:02 p.m., the video records a sound consistent with one gunshot. At approximately 8:44:30 p.m., what appears to be a pickup truck leaves the general area of Scraper's residence.

27. After the Adair County Sheriff's office responded to the scene, MATLOCK was seen walking down the road toward the residence.

28. MATLOCK told Adair County deputies and others near the residence that he "wrecked his truck." MATLOCK also told an Adair County deputy to pull out the deputy's firearm and kill MATLOCK "[b]ecause all the death I've caused tonight would have been for no reason." Later, MATLOCK stated the following while talking to himself: "Larry is gone now and Bob is gone. Bob is evil." Scraper often went by "Bob."

29. MATLOCK's truck was found at a church parking lot approximately one-half mile from the residence. The buttstock of a firearm was in plain view in the backseat area. The vehicle was secured, transported to the Adair County Sheriff's office, and searched pursuant to a search warrant. A Remington model 700 rifle (bolt action) with a Nikon scope was recovered.

30. On September 20, 2021, a phone was seized pursuant to a federal search warrant executed on MATLOCK's Dodge Ram pickup truck. The seized phone is an Android cellular telephone associated with telephone number 918-507-2644. MATLOCK identified that telephone number as his number. Open source records indicate Verizon is the current service provider for the stated cellular number. Location and other data requested from Google for the time period specified in Attachment B are likely to constitute evidence related to the aforementioned crime.

31. Scraper's residence is located on a gravel road in an apparently low-traffic area. The only other known residence located on the gravel road is Scraper's brother's house. Across

the gravel road from Scraper's brother house is a small business located in a mobile home trailer and workshop. A residential or commercial structure is located on the east side of the business trailer. Just south of Scraper's brother's house, the road makes a sharp turn to the east and leads to Scraper's residence. No other residences or businesses are located on this eastward stretch of gravel road (East 823rd Road) where Scraper's residence is located.

32. The requested location, shown in attachment A, is limited to an approximate 250-meter area around a specific location, on a specific date, during a very narrow timeframe in which criminal activity occurred. By providing the very limited area, on a known date, during a known criminal activity timeframe, it is highly likely investigators will be able to obtain the most limited information possible, while still identifying potential Subject unique IDs from Google for further follow-up.

33. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Location described in Attachment A during the time period described in Attachment A for evidence of the crime(s) at issue in this case. The information to be searched includes: (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

34. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Section I of Attachment B:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Location described in Attachment A during the time

period described in Attachment A. For each device, Google will provide an anonymized identifier, known as a Reverse Location Obfuscation Identifier ("RLOI"), that Google creates and assigns to a device for purposes of responding to this search warrant. Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e,.* "maps display radius"), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, Bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.,* example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

35. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

CONCLUSION

36. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to Title 18, United States Code, Section 2703(c) and Federal Rule of Criminal Procedure 41.

37. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Christopher Worshek, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on October 22, 2021.

UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF OKLAHOMA

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC and applies to:

(1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.,* "maps display radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

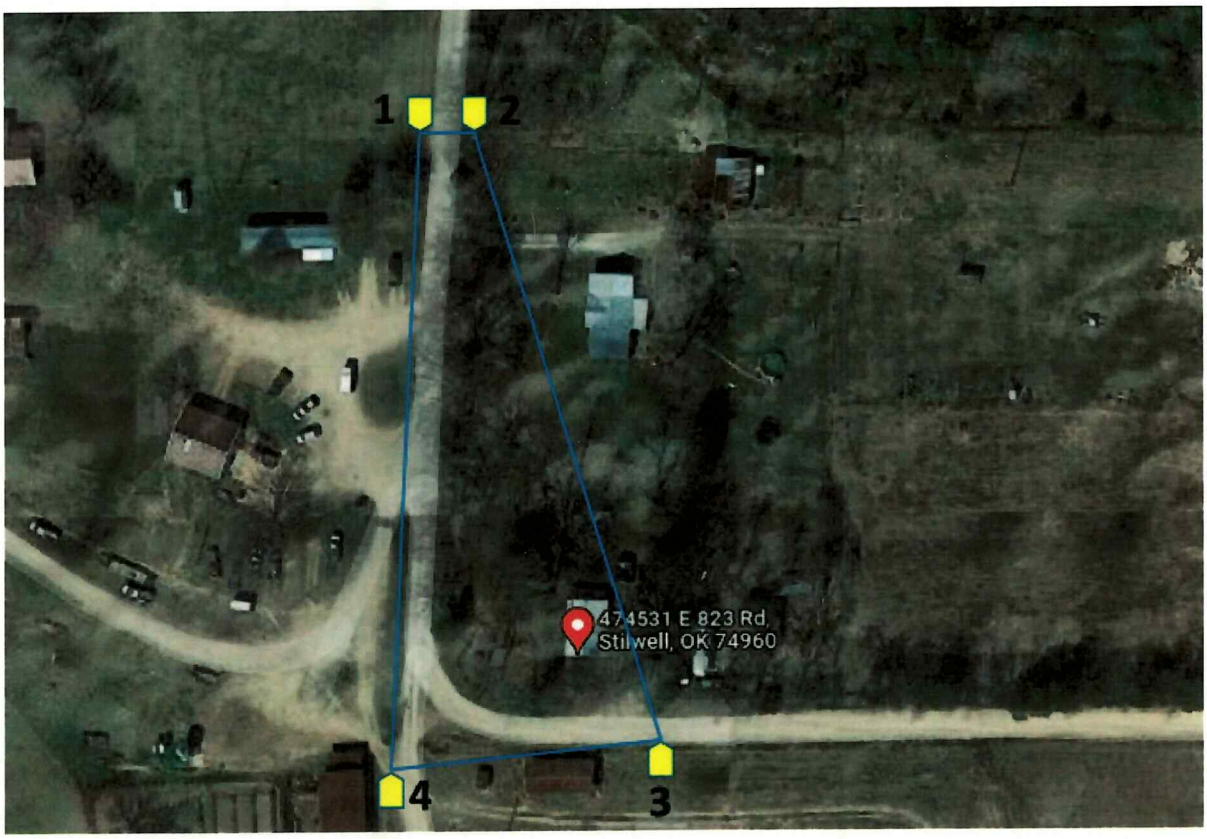
(2) identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

Polygon

- Date: September 14, 2021
- Time Period (including time zone): 2020 - 2050 CST
- Target Location: Geographical area identified as a polygon defined by Point 1: **[35.824093, -94.568288],** Point 2: **[35.824094, -94.568174],** Point 3: **[35.822942, -94.567721],** Point 4: **[35.822913, -94.568348]**

Visual Depiction of Location



ATTACHMENT B

Particular Items to be Seized

I. Information to be Disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.

3. Google shall disclose to the government identifying information, as defined in Title 18, United States Code, Section 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence of a violation of Title 18, United States Code, Sections 1111(a), 1151, and 1153 (Murder in Indian Country).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.